I. AMENDMENTS

IN THE DRAWINGS:

This application consists of formal Figures 1-12, shown on eight pages. Figure 12 has been amended. Attached is a Letter to Official Draftsman transmitting a copy of informal Figure 12, as filed, showing proposed amendment. Applicants respectfully request to delete informal Figure 12 and replace with formal Figure 12, as amended.

Applicants also submit formal Figures 1-12.

IN THE SPECIFICATION:

1.0 On Page 9, the paragraph beginning on Line 2 has been rewritten as follows:

Referring initially to Figure 1, illustrated is a block diagram of a computer system 150 employing an access token 100. The computer system 150 is illustrated as having a central processing unit (or "CPU") 160, a nonvolatile storage device 195 such as an ATA-3 type hard disk drive (or "HDD"), and an 8051 micro-controller 170. CPU 160 is shown receiving CMOS settings 180 from an area of nonvolatile memory, while the 8051 micro-controller 170 is shown receiving data from nonvolatile memory 190. Access token reader 120 is shown reading access token 100 and providing data to CPU 160 while password or access code 130 is shown entered into input device 140 and transmitted to micro-controller 170. Micro-controller 170 determines if access code 130 is correct and returns a "true" or "false" to CPU 160.

a1

2.0 On Page 9, the paragraph beginning on Line 28 has been rewritten as follows:

When a person places the access token 100 on the access token reader 120, security software within computer system 150 is invoked and prompts the user to enter the PIN number 130 on an input device 140. The security software program code may be embedded within the basic input-output system that is stored along with the CMOS settings 180 in nonvolatile memory within computer system 150. In this way, the BIOS may operate without exposing data on nonvolatile storage device 195. In one example, the input device 140 is a keyboard upon which the user enters a PIN number. In another example, the input device

a2

140 is a biometric reader that reads biometric data from the user. In a specific example, biometric data is a fingerprint and an input device 140 is a fingerprint reader. Another example of biometric data is eye retina data that is read with an eye scanner. Another example of biometric data is voice data that is spoken into an input device 140, such as a microphone, and compared with a voice print of the user.

a2

3.0 On Page 31, the paragraph beginning on Line 8 has been rewritten as follows:

Figure 12 shows an example of a manufacturer preparing access tokens for a customer 1200. The customer would provide a token request 1201 with policies 1205, an optional group name 1210, and a user password request 1215. Token request 1201 may be for an additional access token for a computer system already received by customer or may be associated with a new computer system request as described in Figure 11 above. Included with the user password request 1215 is the access code 130 shown in Figure 1 containing data the customer desires to use as an access code, or PIN number, associated with the access token. The access code selected by a user could be a PIN number or could include biometric data (i.e., fingerprint data, eye scan data, etc.) the customer wants associated with access token 100. Additionally, the customer may wish to have the manufacturer create a random access code 1225 to include with the access token. After the access code is determined, access token creation 1230 creates the access token by writing the access code to the access token 1235, and writing policies, group name (if desired), and password data to the access token at step 1240. Following creation of the access token, the token 1245 is sent to the customer and the access code 1250 (i.e., PIN number) used to verify ownership the access token is sent to the customer. If the token 1245 was created for an existing computer system used by customer, the access code 1250 is mailed separately from the access token so that an unauthorized person does not receive both the token and the code needed to use the token, thus giving the unauthorized person access to the computer system.

a3